UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT TACOMA

SHIRLEY ELSTON, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

VIRGIN PULSE, INC. AND WELLTOK, INC.,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

TABLE OF CONTENTS

Page

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Plaintiff, SHIRLEY ELSTON (hereinafter, "Plaintiff"), brings this Class Action Complaint against Defendants, VIRGIN PULSE, INC. ("Virgin Pulse"), WELLTOK, INC. ("Welltok") (collectively, "Defendants"), individually, and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. This action arises out of Defendants' failures to safeguard the confidential personal information, Personally Identifying Information[1] ("PII") and Protected Health Information ("PHI")[2] (collectively, "Private Information") of millions of individuals[3], including Plaintiff and the proposed Class Members, resulting in the unauthorized disclosure of that Private Information in a cyberattack in May 2023 to the MOVEit Transfer tool server, including their names, addresses, telephone numbers, email addresses, Social Security Numbers, Medicare/Medicaid ID Numbers,

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d, *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). On information and belief, Welltok and Virgin Pulse are each business associates, and some of the Private Information compromised in the Data Breach is PHI subject to HIPAA.

[3]HipaaJournal, "Welltok Data Breach: 8,493,379 Individuals Affected," https://www.hipaajournal.com/welltok-data-breach/ (last acc. December 18, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

or certain Health Insurance information such as plan or group name, provider names, prescription names, and treatment codes (the "Data Breach").[4]

2. Virgin Pulse is a software development company which holds itself out as "the leading global provider of tech-enabled solutions focused on improving the health and wellbeing of its members."[5]

3. Welltok is a Virgin Pulse subsidiary which provides healthcare providers and insurance plans with online tools to communicate with patients, and which utilizes the MOVEit Transfer tool.[6]

4. This Data Breach is unique in that Plaintiff and the proposed Class Members had no relationship with Virgin Pulse or Welltok, and did not directly provide Defendants with their Private Information.

5. Nevertheless, Defendants came into possession of Plaintiff's and the proposed Class Members' Private Information, on information and belief via their health care providers or plans, and stored this highly sensitive private data in the cloud hosting and file transfer services, the MOVEit file Transfer tool of Progress Software Corporation, a "global data management company serving government agencies, financial service providers, and multiple other industries" across the country and around the world.[7]

---

[4] *See* Welltok, Inc. Notice of Data Security Event, October 24, 2023, available at https://welltoknotice.wpenginepowered.com/?page_id=23 (last acc. December 14, 2023), attached as **Exhibit A** ("Website Data Breach Notice");

Welltok Notice of Data Event to Washington Attorney General, available at https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA27099.pdf (last acc. Dec. 15, 2023), attached as **Exhibit B**;

"Sutter Health Vendor Reports Patient Information Incident," November 3, 2023, available at https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/ (last acc. Dec. 14, 2023).

[5] "Virgin Pulse completes acquisition of Welltok, expanding health engagement capabilities for employers, payers and health systems," Nov. 10, 2021, avail. at https://international.virginpulse.com/press-releases/virgin-pulse-completes-acquisition-of-welltok-expanding-health-engagement-capabilities-for-employers-payers-and-health-systems/ (last acc. Dec. 14, 2023).

[6] *See* Website Data Breach Notice, **Exhibit A**

[7] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

6. Defendants failed to undertake adequate measures to safeguard this Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

7. Although the Data Breach occurred in May 2023, Defendants failed to promptly notify and warn Data Breach victims of the unauthorized disclosure of their Private Information, preventing them from taking necessary steps to protect themselves from injury and harm.

8. As a direct and proximate result of Defendants' failures to protect Plaintiff's and the Class Members' Private Information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

II. PARTIES

9. Plaintiff is a natural person, and resident and citizen of the State of Washington, residing in Spanaway, Washington, in Pierce County, where she intends to remain. Plaintiff is a victim of the Data Breach, and her Private Information has been found on the Dark Web as a result.

10. Defendant VIRGIN PULSE, INC. ("Virgin Pulse") is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located at 75 Fountain Street, Providence, Rhode Island, 02902.[8]

11. Defendant WELLTOK, INC. ("Welltok") is a corporation organized and existing under the laws of the State of Colorado, with its principal place of business located at 75 Fountain Street, Suite 310, Providence, Rhode Island 02902.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom, have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

[8] *See* Virgin Pulse, General Privacy Notice, Sept. 15, 2023, avail. at https://www.virginpulse.com/privacy-notice/

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

13. This Court has personal jurisdiction over Defendants because they conduct substantial business in this jurisdiction and because Plaintiff's claims arise out of or relate to Defendants' contacts with, and conduct within, this District. Further, this Court has general jurisdiction over Defendants PSC and Eversource because their principal places of business are located in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District.

IV. STATEMENT OF FACTS

A. Defendants, Virgin Pulse and Welltok.

15. Headquartered in Providence, Rhode Island, Virgin Pulse is a software development company which represents itself as "…the world's #1 health, wellbeing and navigation platform, […] impact[ing] over 100 million people across 190 countries by helping Fortune 500, national health plans and many other organizations."[9]

16. Virgin Pulse provides companies with software applications for their employees, including a mobile platform aimed at improving employee's health and performance, "cover[ing] all dimensions of wellbeing as the single destination for easy access to benefits, live support, and incentives."[10]

17. Virgin Pulse describes its program as "a voluntary wellness program that encourages healthy lifestyle changes [which] is paid for by your employer, your spouse's employer or other sponsoring organization."[11]

18. In November 2021, Virgin Pulse acquired Welltok, "…the award-winning health activation company," touting that, "[c]ombining Welltok's activation engine with Virgin Pulse's

[9] LinkedIn, Virgin Pulse, avail. at https://www.linkedin.com/company/virgin-pulse/about/ (last acc. Dec. 14, 2023).

[10] https://www.virginpulse.com/solutions/health-and-wellbeing/ (last acc. Dec. 14, 2023).

[11] *See* Virgin Pulse, General Privacy Notice, Sept. 15, 2023, avail. at https://www.virginpulse.com/privacy-notice/

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

daily engagement platform will drive better health outcomes and cost reductions for the companies' combined 4,100 global employer, health plan and health system clients."[12]

19. Welltok is a "Virgin Pulse company [which] operates an online contact-management platform that enables […healthcare clients, including….] Sutter Health to provide patients and members with important notices and communications."[13]

20. According to Welltok, it is:

> …a data-driven, enterprise SaaS company that delivers the healthcare industry's leading consumer activation platform. Welltok's solutions empower health plans, employers, providers, and public entities to connect consumers with personalized health improvement resources, making it easy and rewarding for consumers to complete actions that optimize their health and wellbeing.[14]

21. Welltok provides its communications management platform to numerous healthcare providers and health insurance plans, such as: Sutter Health; Mass General Brigham Health Plan; Asuris Northwest Health; BridgeSpan Health; Blue Cross and Blue Shield of Minnesota and Blue Plus, Blue Cross and Blue Shield of Alabama, Blue Cross and Blue Shield of Kansas; Blue Cross and Blue Shield of North Carolina; CHI Health – NE; CHI Memorial – TN; CHI Memorial – GA, CHI St. Joseph Health; CHI St. Luke's Health Brazosport; CHI St. Luke's Health Memorial; CHI St. Vincent; Corewell Health; Faith Regional Health Services; Horizon Blue Cross Blue Shield of New Jersey; Hospital & Medical Foundation of Paris, Inc. d/b/a Horizon Health; Marshfield Clinic Health System; Mercy Health; Priority Health; Regence BlueCross BlueShield of Oregon; Regence BlueShield; Regence BlueCross BlueShield of Utah; Regence Blue Shield of Idaho; St. Bernards Healthcare; St Joseph Health; St. Alexius Health; St. Luke's Health; Trane Technologies Company LLC and/or group health plans sponsored by Trane Technologies Company LLC or Trane U.S.

---

[12] "Virgin Pulse completes acquisition of Welltok, expanding health engagement capabilities for employers, payers and health systems," Nov. 10, 2021, available at https://international.virginpulse.com/press-releases/virgin-pulse-completes-acquisition-of-welltok-expanding-health-engagement-capabilities-for-employers-payers-and-health-systems/ (last acc. Dec. 14, 2023).

[13] *See* Website Data Breach Notice, **Exhibit A.**

[14] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Inc., Trinity Health; the group health plans of Stanford Health Care, of Stanford Health Care, Lucile Packard Children's Hospital Stanford, Stanford Health Care Tri-Valley, Stanford Medicine Partners, and Packard Children's Health Alliance; the Guthrie Clinic; Virginia Mason Franciscan Health, and others.[15],[16]

22. In providing this contact management tool to its many healthcare clients, Welltok collects its clients' patients' and members' Private Information, Private Information, which Defendants store and transfer using Progress Software Corporation's MOVEit file Transfer tool.

23. Virgin Pulse acknowledges the importance of maintaining the security and privacy of the Private Information it collects, maintaining a Privacy Notice in which it describes the personal information it collects, and promising that, "[w]e are committed to protecting your data and your privacy. To ensure data security, We follow reasonable physical, electronic and managerial procedures designed to safeguard and secure your data and Personal Information."[17]

24. Moreover, in its Privacy Notice, Virgin Pulse states that it protects personal information "during transfers with authorized parties," by "executing appropriate written agreements based on the applicable jurisdiction."[18]

25. Nothing in Virgin Pulse's Privacy Notice permits it to disclose its healthcare client's patients' and members' Private Information to unauthorized third parties as occurred in the Data Breach.

26. Furthermore, Virgin Pulse maintains an "Authorization For Use and Disclosure of Protected Health Information" ("Authorization") posted on its website, which "pertains to your

---

[15] *Id.*

[16] https://healthitsecurity.com/news/8.5m-records-impacted-by-welltok-data-breach-stemming-from-moveit-hack.

[17] *See* Virgin Pulse, General Privacy Notice, last updated Sept. 15, 2023, avail. at https://www.virginpulse.com/privacy-notice/ (last acc. Dec. 18, 2023), attached as **Exhibit C.**

[18] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

right to the privacy of your Protected Health Information (PHI) and relates to participation in the Virgin Pulse Program[,]" on information and belief, including Welltok's programs. [19]

27. Therein, Virgin Pulse states that, "[o]ur Program is administered according to Federal rules, which allow organizations, such as employers, to sponsor wellness programs that seek to improve health or prevent disease."[20]

28. In its Authorization, Virgin Pulse informs users that PHI is "…a special category of Personal Information defined and protected by HIPAA [which] includes individually identifiable information, like your name, combined with medical or health insurance-related information that is collected or maintained on behalf of your health insurance provider or your medical provide."[21]

29. Virgin Pulse promises in the Authorization that:

> Your PHI, including health screening results, health assessment responses and coaching notes, will not be obtained by your Program Sponsor except as described in this Authorization and will not be used by your Program Sponsor for any employment-related purposes. Your PHI will not be sold, exchanged, transferred or otherwise disclosed to third parties for commercial purposes. **Your PHI will not be disclosed except as permitted by this Authorization or Our Privacy Notice, or to the extent permitted by law.** You will not be asked or required to waive the confidentiality of your PHI as a condition of participating in Our Program or receiving an incentive. You may not be discriminated against in employment because of the PHI you provide as part of participating in the wellness program, nor may you be subjected to retaliation if you choose not to participate.
>
> We will only share your PHI with entities that have a legal right to access it, that are obligated to protect it in similar ways that we are obligated to protect it, and that assist in providing Our Program or other health benefits to you…

[19] Virgin Pulse, Authorization For Use and Disclosure of Protected Health Information, last updated December 1, 2023, https://www.virginpulse.com/gina-phi-notice/ (last acc. Dec. 18, 2023), attached as **Exhibit D.**

[20] *Id.*

[21] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

30. Likewise, Welltok acknowledges the importance of maintaining the security and privacy of the Private Information it collects, stating that "[w]e take this event and the security of personal information in our care very seriously."[22]

31. Indeed, Welltok is covered under a Privacy Notice, which was formerly posted to its website—but now is inaccessible as of the date of this Complaint—which states, "[p]rotecting your personal data is important to Welltok and its subsidiaries."[23]

32. In the Privacy Notice, Welltok states:

> When you use any of our websites or mobile applications (the "Platform") or use our and our engagement/customer relationship management platforms and services ("CRM"), we may collect information about you, including information that can be used to identify you ("Personal Information").
>
> Additionally, we may collect Personal Information from your health plan, your employer's self-funded health plan, your employer, a health service provider, your pharmacy and/or other similar types of entities (your "Sponsor") or from other third parties described in this Privacy Notice. In some cases, the Personal Information we collect may include Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act ("HIPAA"), which is a regulated subset of Personal Information. We collect this data to provide you with the services and functionality that you request (the "Services"), as well as for the other purposes described in this Privacy Notice.[24]

33. As detailed in Welltok's Privacy Notice, when users interact with its website or mobile applications ("Platform information") it collects Personal Information including a person's "name; date of birth; email address; home address; business address; phone number; Social Security Number; "Other Identification Numbers (e.g. state-issued identification number, member number, or employee number); Geolocation Data; and Biometric Information; "Other Health Information, [such as] Physical Activity and Movement Data; Health Risk Assessments; Lab Scores; Data Related to Managed Health Programs; Medications and Prescriptions; Cognitive Assessment Data;

---

[22] Website Data Breach Notice, **Exhibit A**.

[23] Welltok, Privacy Notice, effective September 30, 2020, available via the Wayback Machine at https://web.archive.org/web/20220331113739/https://welltok.com/privacy/ (last accessed Dec. 15, 2023), attached as **Exhibit E.**

[24] *Id*.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Health Conditions or Diseases; Health Plan Information; Insurance Information; and Eating Habits and Nutrition[;]" and Protected Health Information "including claims information, lab and biometric information, electronic medical records/electronic health records, and program activity."[25]

34. Therein, Welltok goes onto state, "[w]e limit our use of such information to restrictions imposed by each Sponsor and HIPAA. For more details about the PHI that is provided to us, please review your Sponsor's Notice of Privacy Practices or related disclosures."[26]

35. In its Privacy Notice, Welltok enumerates how it may disclose personal information it collects through the use of the Platform and services, including, *inter alia*:

- Providing services ("Personalize the Services to you; Respond to or fulfill any of your requests; Administer and manage your account; Authenticate your identity; Identify you when you sign in; Provide you with content, including, without limitation, generating recommendations (such as recommended activities, services, benefits, or rewards), and processing your preferences and requests; Track your use of the Services and the progress in the activities in which you participate; Track and prove you with the rewards you earn; Administer newsletters and provide you with information about the Services and activities you have elected to participate in or that may be of interest to you; Administer any contest or promotions, including winner notification and prize delivery; Communicate with you and respond to your questions and requests; and Improve the Platform and Services.");
- Provides services to patients' and members' Sponsors
- ("Administering and managing your Sponsor's wellness program; Providing you with other services on behalf of your Sponsor; Providing you with rewards and incentives that you have earned; Generating analytical reports; and Developing, enhancing, and promoting the Services.");
- Data Aggregation; and, Using De-Identified Aggregated Data for internal purposes, stating that, "[t]o the extent we de-identify and use PHI, we rely upon applicable rules and guidance and under HIPAA. All de-identification of PHI is undertaken pursuant to the safe harbor provisions of the HIPAA Privacy Rule.");
- "[A]s necessary to comply with any applicable laws [;] to prevent or investigate a possible crime, such as fraud or identity theft; to protect the

[25] *Id.*

[26] *Id.*

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

security of our Service; to enforce or apply our online Terms of Use or other agreements; or to protect our own rights or property or the rights, property or safety of our users or others[;]"

- For analytics ("We use analytics, machine learning, and automated decision-making technologies ('Analytics') to support our data processing activities" including "to provide you with recommended activities or content" including for "
- Condition and disease management;
- Weight management;
- Nutrition management;
- Establishing wellness goals;
- Recognizing when you qualify for an award; • Helping you take your medications as instructed; and
- Recommending you visit a doctor, get a screening, or take other affirmative actions"); including to "to help your Sponsor better understand your health, provide tailored recommendations, and generally help you stay healthy…"[27]

36. Ultimately, in its Privacy Notice, Welltok acknowledges, promises, and represents that it will disclose personal information only to certain entities, including: within Welltok's family of businesses; with patients' and members' Sponsors; with Connect Partners; with third-party service providers; and with respect to PHI, specifically states that, "[w]e may provide your PHI to a Sponsor, Connect Partner or third-party service provider as either a covered entity or a business associate. **We will only disclose your PHI as allowed under HIPAA to provide you with the Services or with your express consent**."[28]

37. Moreover, in the Privacy Notice, Welltok details that it may disclose Aggregated Data to "third parties including a Sponsor or a Connect Partner [;] may make de-identified Aggregated Data public on our site[;] publicly, may disclose] information posted to public areas of the Service, including user names; in connection with private messaging; and may disclose personal information "to comply with laws, court orders or subpoenas […;…] to prevent or investigate a

[27] *Id.*

[28] *Id.* (emphasis added).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

possible crime, such as fraud or identity theft; to protect the security of our Service; to enforce or apply our online Terms of Use or other agreements; or to protect our own rights or property or the rights, property or safety of our users or others [; and] in response to a lawful request by public authorities, including to meet national security or law enforcement requirements."[29]

38. In the Privacy Notice, Welltok specifically says:

> In the event that we enter into, or intend to enter into, a transaction that alters the structure of our business, such as a reorganization, merger, sale, joint venture, assignment, transfer, change of control, or other disposition of all or any portion of our business, assets or stock, we may share Personal Information with third parties for the purpose of facilitating and completing the transaction. **If such a transaction occurs, the successor organization's use of your Personal Information will still be subject to this Notice and the privacy preferences you have expressed to us.**[30]

39. Nothing in Welltok's Privacy Notice permits it to disclose its healthcare client's and Sponsors' patients' and members' Private Information to unauthorized third parties as occurred in the Data Breach.

40. In collecting and maintaining Private Information, Defendants agreed they would safeguard the data in accordance with industry standards, internal policies, and state and federal law. After all, Plaintiff and the Class took reasonable steps to secure their Private Information.

41. In addition, Defendants, by and through their agents and employees, represented to patients and members, directly or indirectly, Plaintiff and the proposed Class Members, that Defendants would adequately protect their Private Information and not disclose said information other than as authorized, including as set forth in Virgin Pulse's and Welltok's Privacy Notices.

42. Plaintiff and the proposed Class Members, current and former patients whose Private Information was given by their healthcare providers or plans to Defendants, would not have permitted this information to be given to Defendants in the absence of their promises to safeguard that information, including as set forth in Virgin Pulse's privacy policies.

---

[29] *Id.*

[30] *Id.* (emphasis added).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' Private Information, Defendants assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that they was responsible for protecting their Private Information from unauthorized disclosure.

44. At all times Plaintiff and the members of the proposed Class have taken reasonable steps to maintain the confidentiality of their Private Information; and relied on Defendants to keep their Private Information confidential and securely maintained.

B. Defendants Failed to Safeguard the Private Information of Millions of Patients—the Data Breach

45. Plaintiff and the proposed Class Members are individuals whose PII and PHI, Private Information, was provided to Defendants by their health care providers, plans, or other entities, in connection with Defendants' online contact management platform.

46. As a condition of providing these services, Defendants collected the Private Information of Plaintiff and the proposed Class Members, including but not limited to their names, addresses, telephone numbers, email addresses, Social Security Numbers, Medicare/Medicaid ID Numbers, or certain Health Insurance information such as plan or group name, provider names, prescription names, and treatment codes.[31]

47. In collecting and maintaining Private Information, Defendants implicitly agree that they will safeguard the data using reasonable means according to industry standards, internal policies—their privacy policies—as well as state and federal law.

48. Defendants stored Plaintiff's and the Class Members' Private Information on the MOVEit Transfer server, which Virgin Pulse and/or Welltok used to transfer this data over the internet.

49. On or about May 30, 2023, the Private Information of Plaintiff and the proposed Class Members which was entrusted to Defendants and stored in the MOVEit Transfer tool was

[31] Website Data Breach Notice, **Exhibit A**.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

unauthorizedly disclosed to cybercriminals in the Data Breach, a Clop ransomware or external system breach attack impacting the MOVEit Transfer tool.[32]

50. According to Welltok, as stated in its Data Breach Notice:

> On July 26, 2023, Welltok was alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool.[33]

51. In reality, this "vulnerability" was a cyberattack executed by the notorious Clop ransomware gang, which claimed responsibility, exploiting the MOVEit Transfer and MOVEit Cloud vulnerability for nefarious purposes and exfiltrating Plaintiff's and the proposed Class Members' Private Information. Clop is one of the most active ransomware actors, having breached over 2,000 organizations directly or indirectly in the MOVEit Transfer tool or cloud cyberattacks.[34]

52. According to Welltok, prior to it being alerted in July 2023, it, "…had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the developer of the MOVEit Transfer tool," examined its systems as to vulnerabilities in the MOVEit Transfer server, and "confirmed that there was no indication of any compromise at that time."[35]

53. In truth, on information and belief, Defendants knew of the Data Breach months before on or about May 31, 2023 when Progress Software Corporation posted a notice on its website confirming a SQL injection vulnerability related to its MOVEit Transfer and MOVEit Cloud file transfer services resulting from a breach in its network.[36]

54. Nevertheless, as stated by Welltok, after being alerted in July 2023 to the Data Breach, it continued to investigate with "the assistance of third-party cybersecurity specialists and

---

[32] *Id.*

[33] *Id.*

[34] "Matthew J. Schwartz, Bankinfosecurity.com, "Data Breach Toll Tied to Clop Group's MOVEit Attack Surges," Sept. 25, 2023, avail. at https://www.bankinfosecurity.com/data-breach-toll-tied-to-clop-groups-moveit-attacks-surges-a-23153 (last acc. Dec. 12, 2023).

[35] *Id.*

[36] https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 (last acc. Dec. 15, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

additional information that had been discovered in the intervening period to determine the potential for hidden vulnerabilities on the MOVEit Transfer server and assess the security of data housed on the server," ultimately determining that "….on August 11, 2023 [] an unauthorized actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time" and by, "…August 26, 2023, [] learned that data related to certain individuals was present on the impacted server at the time of the event."[37]

55. The Private Information exfiltrated by cybercriminals in Defendants' MOVEit Data Breach included their names and addresses, telephone numbers, and email addresses; for a small group of impacted clients, Social Security Numbers, Medicare/Medicaid ID Numbers, or certain Health Insurance information such as plan or group names, and for others, certain health information such as a provider names, prescription names, or treatment codes. [38]

56. Defendants, each sophisticated software development companies in the business of collecting, storing, and transmitting sensitive personal data, knew or should have known of the tactics that groups like Clop employ.

57. Although Defendants were aware of the Data Breach at least as of July 26 2023—and likely earlier in May 2023—Welltok waited three (3) months until October 24, 2023 to notify the public, at which time it posted the Notice of Data Privacy Event to its website (Website Data Breach Notice, **Exhibit A**).

58. On information and belief, Welltok made its Data Breach Notice difficult for victims to even find—according to media reports: "While a substitute breach notification was uploaded to the Welltok website in October, it was set as no-index, making it accessible only to those who directly visited the website rather than being discovered through search engines."[39]

---

[37] *Id.*

[38] *Id.*

[39] Raja Wajahat, "Welltok Data Breach: 8.5M US Patients' Information Exposed," Dec. 8, 2023, available at https://securityboulevard.com/2023/12/welltok-data-breach-8-5m-us-patients-information-exposed/ (last acc. Dec. 15, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

59. On November 6, 2023, Welltok reported the Data Breach to the United States Department of Health and Human Services (HHS), Office for Civil Rights, reporting its status as a Business Associate under HIPPA; that the Data Breach was a Hacking/IT Incident to a Network Server; and that 8,493,379 individuals were affected.[40]

60. On November 22, 2023, Welltok reported the Data Breach to the Washington Attorney General, on behalf of Graphic Packaging International, stating that the Data Breach "may have affected the security of certain personal information relating to approximately five hundred fifty-four (554) Washington residents."[41]

61. On November 23, 2023, Welltok reported the Data Breach to the Maine Attorney General, reporting that the breach occurred on May 30, 2023 as a result of an external system breach (hacking) event; that Welltok discovered it on October 23, 2023; that 426,812 person were impacted; and that the information acquired included names or other personal identifiers in combination with Social Security Numbers, dates of birth, treatment information/diagnosis, prescription information, MRN, provider name, treatment cost, and health insurance plan number.[42,43]

62. Further according to Welltok, on November 22, 2023 it began sending written notification of the Data Breach to impacted individuals, *to wit*, for those persons for whom Welltok "operates a voluntary online wellness program that encourages healthy lifestyle changes" for Graphic Packaging International and Premier Health.

63. On December 5, 2023, Welltok made another report of the Data Breach with the Maine Attorney General, this time saying that the Data Breach was discovered on September 22,

---

[40] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last acc. Dec. 18, 2023).

[41] Washington Attorney General, Data Breach Notifications, avail. at https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA27099.pdf (last acc. Dec. 15, 2023), attached as **Exhibit B.**

[42] Maine Attorney General, Data Breach Notifications, available at https://apps.web.maine.gov/online/aeviewer/ME/40/df6b65ea-c8fb-4a62-a5e8-53fec501fabb.shtml (last acc. Dec. 15, 2023).

[43] Welltok Notice of Data Event to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/df6b65ea-c8fb-4a62-a5e8-53fec501fabb/d4837963-13e1-4704-972f-20adaf9d9d5a/document.html (last acc. Dec. 15, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

2023; that 931,316 persons were affected; and providing further written notifications for patients or members of Elixir Pharmacy, OrthoWest, LLC, dba OrthoNebraska Clinics and Nebraska Orthopaedic Hospital LLC, dba OrthoNebraska Hospital ("OrthoNebraska"), and OSF HealthCare System.[44]

64. As follows below, Defendants have failed to notify *all* individuals whose Private Information was compromised in the Data Breach, including Plaintiff.

65. In the Data Breach Notices, Welltok vaguely described the Data Breach and went onto say that, "[w]hile we have no evidence that any of your information has been misused, we are notifying you and providing information and resources to help protect your personal information."[45]

66. Despite the foregoing, Welltok encouraged Data Breach victims to "remain vigilant against incidents of identity theft and fraud by regularly reviewing [] account statements and monitoring [] free credit reports for suspicious activity and to detect errors," and informed them of their abilities to place a fraud alert on their credit files, place a credit freeze on their credit reports, and offered them Experian IdentityWorks credit monitoring for 12 or 24 months.[46]

67. Contrary to their duties and alleged commitments to safeguard Private Information, Defendants did not in fact follow industry standard practices in securing patients' and members' Private Information, as evidenced by the Data Breach.

68. Defendants failed to adequately protect the Private Information of those patients and members of their healthcare clients whose personal, private data was entrusted to them, Plaintiff and the proposed Class Members, which Defendants stored in the MOVEit Transfer tool server and/or on their networks.

69. Defendants failed to use adequate cybersecurity measures to protect Plaintiff's and the proposed Class Members' Private Information, and failed to adequately train employees on

---

[44] Maine Attorney General, Data Breach Notifications, available at https://apps.web.maine.gov/online/aeviewer/ME/40/adf9bbf8-f167-4c1e-94ab-79c7ec810da1.shtml.

[45] *See* Website Data Breach Notice, **Exhibit A**.

[46] *See id*.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

reasonable cybersecurity protocols, causing the Private Information to be unauthorizedly disclosed in the Data Breach.

70. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, any credit monitoring and identity theft protection which Defendants have or may offer is wholly insufficient to compensate Plaintiff and the Class Members for their injury and damages resulting therefrom.

71. Indeed, as a result of the Data Breach which Defendants permitted to occur by virtue of their inadequate data security practices, Plaintiff and the proposed Class Members have suffered widespread and severe injury and damages, as set forth herein.

C. The Data Breach was a Foreseeable Risk of which Defendants Were on Notice.

72. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the file-transfer software industry preceding the date of the breach, including recent similar attacks against secure file transfer companies like Accellion and Fortra carried out by the same Russian cyber gang, Clop.[47]

73. In light of recent high profile data breaches at other file-transfer software companies, Defendants knew or should have known that their electronic records and healthcare clients' patients' and members' Private Information would be targeted by cybercriminals.

74. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[48] The 330 reported

[47] *See* https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomwaregang/ (last visited on June 21, 2023); see also https://www.bleepingcomputer.com/news/security/fortra-sharesfindings-on-goanywhere-mft-zero-day-attacks/ (last visited on June 21, 2023).

[48] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[49]

75. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain Private Information." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [50]

76. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Virgin Pulse.

D. Plaintiff's Experience

77. Plaintiff is unaware how Defendants obtained her Private Information, but on information and belief, Welltok and/or Virgin Pulse may have obtained her said information from her husband's health insurance company, BlueCross BlueShield of Illinois.

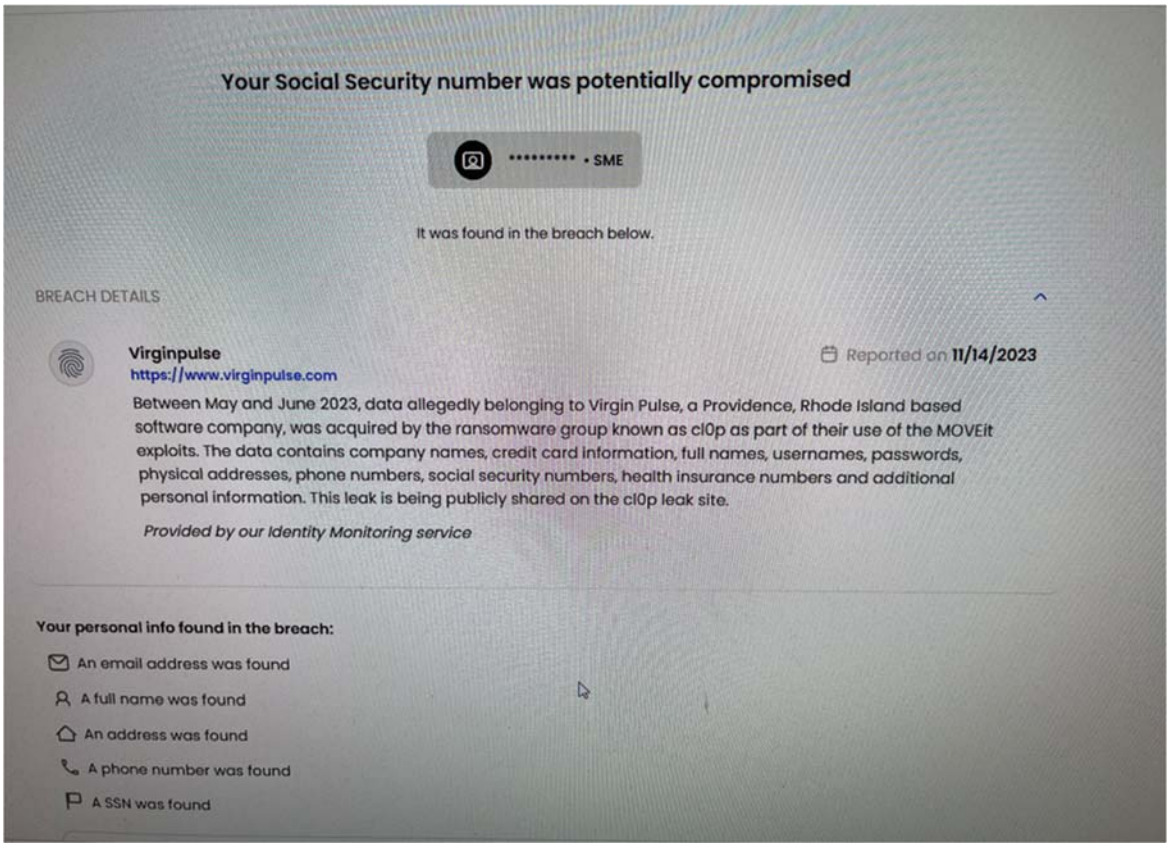
78. On information and belief, Defendants collected Plaintiff's Private Information, including her full name, address, Social Security Number, telephone number, and email address, which they stored on their MOVEit Transfer tool server and/or in their information technology networks.

79. Plaintiff was alerted to her Private Information being unauthorizedly disclosed in the Data Breach on or about November 14, 2023, by her McAfee security identity monitoring service, which showed that her full name, address, Social Security Number, telephone number, and email address were found in the Virgin Pulse Data Breach, and is on the Dark Web as publicly shared on the leak website of the cybercriminals:

[49] *Id.*

[50] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX



80. On information and belief, Virgin Pulse has not independently notified the public of the Data Breach, but Welltok has now done so via its Website Data Breach Notice (**Exhibit A**) and in mailed notices to some Data Breach victims.

81. Despite her Private Information having been found on the Dark Web as a result of the Data Breach, Plaintiff has not received any written notification from Defendants.

82. As a direct and proximate result of the Data Breach that Defendants permitted to occur, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including, but not limited to:

a. her Private Information being published on the Dark Web, where it has and will be used for illegal and fraudulent purposes and sold to other criminals;

b. fraudulent attempts by criminals having knowledge of her name, address, and financial credit union account information attempting to collect a fraudulent payday loan debt taken out in May 2012 for $4,071.00 which she does not owe, and for which she filed a complaint with the Washington Attorney General and the FTC Consumer Financial

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

Protection Bureau, who confirmed it was a scam. As a result, Plaintiff contacted her credit union and closed the account;

c. voluminous spam telephone calls and emails, including phishing scams, since Summer, 2023, shortly after the May 2023 Data Breach.

83. Further, as a result of the Data Breach, Plaintiff has, and will, spend time dealing with its consequences, including time spent ascertaining how Defendants came into possession of her Private Information; self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred; closing her accounts; instituting a credit freeze on her credit file; time to report spam phishing emails to her email service provider to block future attempts, and forcing her to change her email provider; time on the telephone with criminals attempting to perpetrate a fraud; and time filing consumer complaints. This time has been lost forever and cannot be recaptured.

84. As a result of the Data Breach, Plaintiff has experienced feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

85. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that was entrusted to Defendants, which was compromised in and as a result of the Data Breach.

86. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and criminals.

87. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

E. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

88. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendants.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

89. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered and will continue to suffer damages, including unauthorized disclosure of this Private Information onto the Dark Web, monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Private Information in their possession.

90. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

91. The value of Plaintiff's and the Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen Private Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

92. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

93. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

94. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

95. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

96. Defendants disclosed the Private Information of Plaintiff and the Class to an unknown vendor who failed to take adequate measures to safeguard that Private Information, which was unauthorizedly disclosed in the Data Breach for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Private Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

97. Defendants' failure to promptly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

F. Defendants failed to adhere to FTC guidelines.

98. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

99. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[51]

100. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[52]

[51] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

[52] *See id*.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

101. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

102. These FTC enforcement actions include actions against entities failing to safeguard Private Information such as Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

103. Defendants failed to implement basic data security practices widely known throughout the industry.

104. Defendants' failures to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitute an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

105. Defendants were at all times fully aware of their obligations to protect the Private Information of current and former patients and members that was entrusted to them. Defendants were also aware of the significant repercussions that would result from their failure to do so.

G. Defendants Fail to Comply with Industry Standards

106. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

107. Several best practices have been identified that a minimum should be implemented by businesses in possession of PII/Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

108. Other best cybersecurity practices that are standard for businesses holding PII include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

109. Defendants failed to ensure that the MOVEit Transfer tool servers or other networks met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

110. These foregoing frameworks are existing and applicable industry standards for businesses' obligations to provide adequate data security for those individuals whose Private Information they collect and maintain. Upon information and belief, Defendants failed to ensure that their systems complied with at least one–or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

V. CLASS ACTION ALLEGATIONS

111. Plaintiff sues individually on behalf of herself, and on behalf of the proposed class ("Class"), defined as follows, pursuant to CR 23:

> **All persons whose Private Information was compromised in Defendants' Data Breach and MOVEit vulnerability.**

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

112. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

113. Plaintiff reserves the right to amend the class definition.

114. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under CR 23(a):

a. **Numerosity**. Plaintiff is representative of the Class, consisting of potentially millions of members, far too many to join in a single action;

b. **Ascertainability**. Class Members are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendants breached contractual promises to safeguard Plaintiff's and the Class's Private Information;

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Data Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, or injunctive relief.

115. Further, pursuant to CR 23(b)(3), common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual Plaintiff are insufficient to make individual lawsuits economically feasible.

116. In addition, this action is properly certified as a class action under CR(b)(2) as Defendants have acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

FIRST CLAIM FOR RELIEF

NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

117. Plaintiff realleges all previous paragraphs as if fully set forth below.

118. Plaintiff and the Class Members entrusted their Private Information to Defendants. Defendants owed to Plaintiff and other Class Members a duty to exercise reasonable care in handling and using the Private Information in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect, secure and safeguard the Private Information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, as transpired in the Data Breach, and to promptly detect attempts at unauthorized access.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

119. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that their failure to adequately safeguard their Private Information in accordance with state-of-the-art industry standards concerning data security, and the applicable standards of care from statutory authority like HIPAA and Section 5 of the FTC Act, would result in the compromise of that Private Information—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members's Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

120. Further, Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their healthcare clients' patients and members, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law. Defendants were in a position to ensure that their systems and MOVEit servers were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach. Plaintiff and Class Members reasonably believed that Defendants would take adequate security precautions to protect their Private Information.

121. Defendants' duties to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

122. In addition, Defendants each had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

123. Defendants' duties to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

124. Further still, Defendants owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendants also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

125. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and Class Members's Private Information.

126. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants hold vast amounts of Private Information, it was "inevitable" that unauthorized individuals would attempt to access Defendants' databases containing the Private Information—whether by malware or otherwise.

127. Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

128. Defendants breached their duties of care owed to the Plaintiff and the Class members by failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information; by failing to adequately monitor the security of their networks and systems; and by failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

129. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class members' Private Information.

130. Moreover, Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members's injury.

131. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members's injuries-in-fact.

132. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

133. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation: unauthorized disclosure of their Private Information and publication onto the Dark Web; monetary losses; lost time; anxiety, and emotional distress; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; continued risk to their Private Information, which

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Private Information in their possession; and increased risk of harm.

134. As a result of Defendants' ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

135. As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

136. Plaintiff seeks the award of actual and compensatory damages on behalf of herself and the Class, to compensate them for the harm caused by the Data Breach, resulting directly from Defendants' negligence as set forth herein; as well as punitive damages, as permitted by law.

SECOND CLAIM FOR RELIEF

BREACH OF AN IMPLIED CONTRACT (ON BEHALF OF PLAINTIFF AND THE CLASS)

137. Plaintiff incorporates the above allegations as if fully set forth herein.

138. Defendants required Plaintiff and Class Members to entrust them with their Private Information, directly or indirectly through Plaintiff's and Class Members' health insurance providers or plans, in order for Defendants to provide their health communications platforms.

139. In turn, and through internal policies set forth herein, Defendants agreed they would safeguard and not disclose the Private Information they collect to unauthorized persons.

140. Plaintiff and the Class Members accepted Defendants' offer by providing Private Information to Defendants in exchange Defendants' services.

141. Implicit in the parties' agreement was that Defendants would adequately safeguard the Private Information entrusted to them and would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

142. Plaintiff and the Class Members would not have entrusted their Private Information to Defendants in the absence of such agreement with Defendants.

143. Defendants materially breached the contract(s) they had entered into with Plaintiff and Class Members by failing to safeguard such Private Information and failing to notify them promptly of the intrusion into their computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiff and Class Members by:

A. Failing to properly safeguard and protect Plaintiff's and Class Members's Private Information;

B. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

C. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendants created, received, maintained, and transmitted.

144. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendants' material breaches of their agreement(s).

145. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

146. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

147. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

148. Defendants knew or should have known that Plaintiff and Class members reasonably understood that Defendants would safeguard the Private Information Defendants required Plaintiff

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

and Class Members to disclose in order for Defendants provide communications platform services to Plaintiff's and the Class's healthcare providers or plans. Despite Plaintiff's and Class Members' reasonable expectations, Defendants failed to implement appropriate cybersecurity protocols to protect the Private Information on their systems from the Data Breach.

149. Defendants failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

150. In these and other ways, Defendants violated their duties of good faith and fair dealing.

151. Plaintiff and Class Members have sustained injury and damages because of Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing, including, without limitation: including, without limitation: unauthorized disclosure of their Private Information and publication onto the Dark Web; monetary losses; lost time; anxiety, and emotional distress; loss of the opportunity to control how their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Private Information in their possession; increased risk of harm; and lost benefit of the bargain.

THIRD CLAIM FOR RELIEF

UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

152. Plaintiff incorporates the above allegations as if fully set forth herein.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

153. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

154. Plaintiff and Class Members conferred a benefit upon Defendants, directly or indirectly, by paying monies to Defendants, a portion of which was for adequate data security, and by providing their valuable Private Information to Defendants. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff and Class Members.

155. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their Private Information because Defendants failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information or paid monies to Defendants, directly or indirectly, for their communications platform services had they known Defendants would not adequately protect their Private Information.

156. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of their misconduct and Data Breach.

FOURTH CLAIM FOR RELIEF

VIOLATION OF THE WASHINGTON DATA BREACH DISCLOSURE LAW (ON BEHALF OF PLAINTIFF AND THE CLASS)

157. Plaintiff incorporates all previous paragraphs as if fully set forth below.

158. RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

159. The Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendants, leading to a "breach of the security of [Defendants'] systems," as defined by RCW § 19.255.010.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

160. Defendants failed to disclose that the Private Information of millions of their healthcare clients' patients and members had been compromised "immediately" upon discovery—although Welltok and/or Virgin Pulse discovered the Data Breach at least as early as July 2023, they waited three (3) months until October 24, 2023 to notify the public via the Website Data Breach Notice; waited until November 22, 2023 to send *some* affected persons direct written notice; and Defendants have failed to notify some affected individuals, such as Plaintiff, at all. In so doing, Defendants unreasonably delayed informing Plaintiff and the proposed Class about the Data Breach.

161. Plaintiff and the proposed Class were damaged as a direct and proximate result of Defendants' failure to provide timely notice, as set forth herein.

FIFTH CLAIM FOR RELIEF

VIOLATION OF THE WASHINGTON STATE CONSUMER PROTECTION ACT (RCW 19.86.010, *ET SEQ.*) (ON BEHALF OF PLAINTIFF AND THE CLASS)

162. Plaintiff incorporates all previous paragraphs as if fully set forth below.

163. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

164. Defendants are each a "person" as described in RWC 19.86.010(1).

165. Defendants engage in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

166. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

167. In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

168. Defendants also violated the CPA by failing to timely notify and concealing from Plaintiff and Class members the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

169. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

170. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

171. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, including, without limitation: unauthorized disclosure of their Private Information and publication onto the Dark Web; monetary losses; lost time; anxiety, and emotional distress; loss of the opportunity to control how

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

their Private Information is used; diminution in value of their Private Information; compromise and continuing publication of their Private Information; Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; continued risk to their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Private Information in their possession; and increased risk of harm.

172. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

173. Plaintiff, on behalf of herself and the Class Members also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiff, on behalf of herself and the Class Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

SIXTH CLAIM FOR RELIEF

INVASION OF PRIVACY
(ON BEHALF OF THE PLAINTIFF AND CLASS)

174. Plaintiff incorporates all previous paragraphs as if fully set forth below.

175. Defendants publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and Class Members by

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

disclosing and exposing Plaintiff's and Class Members' private and sensitive PHI and PII—Private Information—to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the Dark Web and elsewhere.

176. Plaintiff's and Class Members' Private Information, which includes their names, addresses, telephone numbers, email addresses, Social Security Numbers, Medicare/Medicaid ID Numbers, or certain Health Insurance information such as plan or group name, provider names, prescription names, and treatment codes, was private and intimate.

177. Defendants' disclosure of the Private Information unreasonably, substantially and seriously interfered with Plaintiff's and Class members' privacy and ordinary sensibilities. Defendants should appreciate that the cyber-criminals who stole the Private Information would further sell and disclose it as they are doing and as they did. That the original disclosure is devastating to Plaintiff and Class members even though it may have originally only been made to one person or a limited number of cyber-criminals does not render it any less a disclosure to the public-at-large—especially given the publication of that Private Information on the Dark Web.

178. The tort of public disclosure of private facts is recognized in Washington. Plaintiff's and Class members' private and sensitive Private Information was publicly disclosed by Defendants in the Data Breach with reckless disregard for the offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendants knew that Plaintiff's and Class Members' Private Information is not a matter of legitimate public concern.

179. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been injured and are entitled to damages, as set forth herein.

PRAYER FOR RELIEF

Plaintiff, SHIRLEY ELSTON, individually, and on behalf of all others similarly situated, demands a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

HAGENS BERMAN
1301 Second Avenue, Suite 2000, Seattle, WA 98101
(206) 623-7292 OFFICE (206) 623-0594 FAX

B. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Enjoining Defendants from further deceptive practices and making untrue statements about their data security, the Data Breach, and the stolen Private Information;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

DATED this 2nd day of February, 2024.

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By: */s/ Sean R. Matt*

Sean R. Matt (WSBA No. 21972)
1301 Second Avenue, Suite 2000
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
sean@hbsslaw.com

J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)
Andrew E. Mize (*Pro Hac Vice* forthcoming)
STRANCH, JENNINGS, & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com

Attorneys for Plaintiff